

IN THE CLAIMS:

1. (currently amended) A method for scan to confidential print job communications, the method comprising:

- at a source, scanning a document;
- accepting a password;
- encrypting the scanned document, creating an encrypted document;
- transmitting a file including a header with an unencrypted identification of the encrypted document, the password, and the encrypted document, from the source to a network-connected printer;
- at the printer, accepting the file from the source;
- storing the encrypted document in printer memory until a user enters an access code;
- accepting the access code from the user at a printer local interface;
- comparing the access code to the password in the file;
- in response to a matching the access code to the password, decrypting the encrypted document; and,
- printing the decrypted document.

2. canceled

3. (original) The method of claim 1 wherein accepting a password includes accepting a password selected from the group including a PIN number, an alphanumeric code, biometric data, Smart card, magnetic stripe card, and proximity badge.

4. (previously presented) The method of claim 1 wherein encrypting the scanned document includes:

at the source, deriving an encryption key from the password;
and,
using the encryption key to encrypt the document.

5-6. canceled

7. (previously presented) The method of claim 1 further comprising:

at the source, hashing the password;
at the printer, hashing the access code; and,
wherein comparing the access code to the password includes
comparing the hashed password to the hashed access code.

8. (previously presented) The method of claim 1 wherein decrypting the document includes:

regenerating the encryption key from the access code; and,
using the encryption key to decrypt the encrypted document.

9. canceled

10. (previously presented) A scan to confidential print job communications system, the system comprising:

a scanner having an input to accept a paper media document and a user interface to accept a password, the scanner scanning the document, encrypting the scanned document, and transmitting a file including a header with an unencrypted identification of the encrypted document and the password, along with the encrypted document, on a network-connected output; and,

a printer having a network-connected input to accept the file from the scanner, the printer using the header to identity the encrypted document and store the encrypted document in memory until a user enters an access code, the printer having a local user interface to accept the access code from the user, the printer comparing the access code to the password, and in response to a matching the access code to the password, decrypting the encrypted document and supplying a printed copy of the decrypted document.

11. canceled

12. (original) The system of claim 10 wherein the scanner user interface accepts a password selected from the group including a PIN number, an alphanumeric code, biometric data, Smart card, magnetic stripe card, and proximity badge.

13. (previously presented) The system of claim 10 wherein the scanner includes an encryption unit having an input to accept the scanned document and an input to accept the password, the encryption unit deriving an encryption key from the password and using the encryption key to supply the encrypted document at an output.

14-15. canceled

16. (previously presented) The system of claim 10 wherein the scanner sends a file header with a hashed password; and,

wherein the printer includes a hash unit with an input to accept the access code and an input to accept the hashed codeword, the hash unit generating a hashed access code and supplying a decision at an output in response to comparing the hashed password to the hashed access code.

17. (original) The system of claim 16 wherein the printer further includes a decryption unit having an input to accept the decision from the printer hash unit, an input to accept the encrypted document, and an input to accept the access code, the decryption unit regenerating the encryption key from the access code and using the encryption key to supply the decrypted document at an output.

18. (previously presented) The system of claim 10 wherein the printer user interface accepts an access code selected from the group including a PIN number, an alphanumeric code, biometric data, Smart card, magnetic stripe card, and proximity badge.

19. canceled